CLAIMS

What is claimed is:

1. A method of determining an error correction parameter for use in Montgomery modular processing, comprising:

(a) performing a modulo operation on a modulus value by sequentially performing a plurality of shift/compare operations on contents of a working register; and

(b) storing an initial value in the working register that is greater than the modulus value.

2. The method of claim 1, further comprising determining the initial value by left shifting the contents of the working register a number of positions correlating to one position past a most significant bit of the modulus value.

3. The method of claim 1, further comprising determining a most significant bit of the modulus value.

4. The method of claim 3, further comprising checking each word of the modulus value for the most significant bit.

5. The method of claim 1, further comprising determining the initial value while the modulus value loads.

6. The method of claim 1, wherein performing the plurality of shift/compare operations further comprises left shifting the working register to determine a shifted result.

7. The method of claim 6, further comprising processing the modulus value and the shifted result using bit-by-bit subtraction to determine a subtracted result.

8. The method of claim 7, further comprising determining a next working value from among a group consisting of the shifted result and the subtracted result by comparing the subtracted result to zero.

9. The method of claim 7, further comprising storing the shifted and subtracted results in separate memories.

10. The method of claim 1, wherein performing the plurality of shift/subtract operations further comprises left shifting the working register a plurality of positions in a single loop iteration.

11. The method of claim 10, further comprising left shifting the working register a number of positions corresponding to a number correlating to a difference between a most significant bit of the working register and a most significant bit of the modulus value.

12. The method of claim 1, further comprising conducting in parallel a shift function and a subtraction function of a shift/compare operation of the plurality of shift/compare operations.

13. A method of determining an error correction parameter used in Montgomery modular processing, comprising:

(a) performing a modulo operation by sequentially performing a plurality of shift/compare operations on contents of a working register; and

(b) selectively shifting contents of the working register by more than one position in connection with a shift/compare operation.

14. The method of claim 13, wherein selectively shifting further comprises left shifting the working register a number of positions corresponding to a difference between a most significant bit of the working register and a most significant bit of a modulus value.

15. The method of claim 14, wherein the left shifting further comprises determining the most significant bit of the working register.

16. The method of claim 13, further comprising conducting a subtraction function of a shift/compare operation of the plurality of shift/compare operations in parallel with selectively shifting the contents of the working register.

17. A circuit arrangement, comprising:

(a) a working register; and

(b) an error correction parameter circuit configured to determine an error correction parameter for use in Montgomery modular processing by performing a modulo operation on a modulus value, wherein the error correction parameter circuit is configured to

perform the modulo operation by sequentially performing a plurality of shift/compare operations on contents of the working register, wherein the error correction parameter circuit is further configured to store an initial value in the working register that is greater than the modulus value.

18. The circuit arrangement of claim 17, wherein the initial value correlates to a working register value of one position past a most significant bit of the modulus value.

19. The circuit arrangement of claim 17, wherein the error correction parameter circuit further comprises a state machine configured to determine a most significant bit of the modulus value.

20. The circuit arrangement of claim 19, wherein the state machine checks each word of the modulus value for the most significant bit.

21. The circuit arrangement of claim 17, wherein the error correction parameter circuit further comprises a variable shifter configured to left shift the working register to produce a shifted result.

22. The circuit arrangement of claim 21, wherein the error correction parameter circuit further comprises a subtraction circuit configured to process the modulus value and the shifted result using bit-by-bit subtraction to determine a subtracted result.

23. The circuit arrangement of claim 22, wherein the error correction parameter circuit further comprises a state machine configured to determine a next working value from among a group consisting of the shifted result and the subtracted result by comparing the subtracted result to zero.

24. The circuit arrangement of claim 22, wherein the error correction parameter circuit further comprises a plurality of registers for separately storing the shifted and subtracted results.

25. The circuit arrangement of claim 17, wherein the error correction parameter circuit further comprises a variable shifter configured to shift the working register a plurality of spaces in a single loop iteration.

26. A program product comprising hardware definition program code defining the circuit arrangement of claim 17, and a signal bearing medium bearing the hardware definition program code, wherein the signal bearing medium comprises at least one of a transmission medium and a recordable medium.

27. The circuit arrangement of claim 17, wherein the plurality of shift/compare operations include a shift function and a subtraction function executed in parallel.

28. A circuit arrangement, comprising:

(a) a working register; and

(b) an error correction parameter circuit configured to determine an error correction parameter for use in Montgomery modular processing by performing a modulo operation on a modulus value, wherein the error correction parameter circuit is configured to perform the modulo operation by sequentially performing a plurality of shift/compare operations on contents of the working register, wherein the error correction parameter circuit comprises a variable shifter configured to selectively shift contents of the working register by more than one position in connection with a shift/compare operation.

29. The circuit arrangement of claim 28, wherein the variable shifter selectively shifts the contents of the working register a number of positions corresponding to a difference between a most significant bit of the working register and a most significant bit of a modulus value.

30. A program product comprising hardware definition program code defining the circuit arrangement of claim 28, and a signal bearing medium bearing the hardware definition program code, wherein the signal bearing medium comprises at least one of a transmission medium and a recordable medium.

31. The circuit arrangement of claim 28, wherein the plurality of shift/compare operations include a shift function and a subtraction function executed in parallel.